UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/753,229	12/28/2000	Darwin A. Engwer	3239P065	9332

8791 7590 07/16/2004

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD, SEVENTH FLOOR
LOS ANGELES, CA 90025

EXAMINER	
SHERKAT, AREZOO	

ART UNIT	PAPER NUMBER
2131	8

DATE MAILED: 07/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/753,229	ENGWER ET AL.	
	Examiner	Art Unit	
	Arezoo Sherkat	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 December 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 December 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-28 are presented for examination.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-8, 11-19, and 21-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Kimura, (U.S. Publication No. 2001/0048744 and Kimura hereinafter).

Regarding claims 1 and 27, Kimura discloses an authentication method comprising:

generating an initialization vector at a first electronic device, determining at the first electronic device whether the initialization vector falls within a first group of initialization vectors, the first group includes a plurality of initialization vectors solely used in connection with an authentication sequence, and encrypting information using in part the initialization vector for return to a second

electronic device if the initialization vector falls within the first group (Pages 3-4, Par. 0037-0040).

Regarding claim 2, Kimura discloses wherein the first electronic device is a wireless unit (Page 2, Par. 0019).

Regarding claim 3, Kimura discloses wherein the second electronic device is an access point (Page 2, Par. 0019).

Regarding claim 4, Kimura discloses wherein prior to generating the initialization vector, the method comprises receiving the information from the second electronic device by the first electronic device (Pages 3-4, Par. 0037-0040).

Regarding claim 5, Kimura discloses wherein the information is a challenge text (Pages 3-4, Par. 0037-0040).

Regarding claim 6, Kimura discloses wherein the challenge text is a first sequence of bits and the initialization vector is a second sequence of bits produced by a number generator (Page 4-5, Par. 0048-0051).

Regarding claim 7,Kimura discloses wherein the number generator is a pseudo-random number generator (Page 3-4, Par. 0039 and 0049).

Regarding claim 8, Kimura discloses further comprising regenerating an initialization vector if the initialization vector fails to fall within the first group (Page 4-5, Par. 0047-0052).

Regarding claims 11 and 18, Kimura discloses wherein prior to receiving the challenge text, the method further comprises negotiating a shared secret key between the first electronic device and the second electronic device (i.e., shared secret data)(Pages 3-4, Par. 0037-0040).

Regarding claims 12 and 19, Kimura discloses wherein the encrypting of the information includes combining the initialization vector with the shared secret key, and repeatedly performing bitwise Exclusive-OR (XOR) operations on the challenge text using a combination of the initialization vector with the shared secret key (Pages 3-4, Par. 0037-0040).

Regarding claim 13, Kimura discloses further comprising: transmitting both the encrypted challenge text and the initialization vector to the second electronic device; decrypting the encrypted challenge text using both the initialization vector and a prestored copy of the shared secret key to recover a challenge text; and comparing the recovered challenge text with the challenge text (Pages 3-4, Par. 0037-0040).

Regarding claim 14, Kimura discloses a method for authenticating a wireless unit in communications with an access point, comprising: transmitting a challenge text from the access point to the wireless unit, receiving an encrypted challenge text and an initialization vector from the wireless unit, decrypting the encrypted challenge text using both the initialization vector and a pre-stored copy of a shared secret key to recover a challenge text, and comparing the recovered challenge text with the challenge text previously transmitted to the wireless unit (Pages 3-4, Par. 0037-0040).

Regarding claim 15, Kimura discloses wherein the challenge text is a first sequence of bits (Pages 3-4, Par. 0037-0040).

Regarding claim 16, Kimura discloses wherein the initialization vector is a second sequence of bits produced by a number generator (Pages 3-4, Par. 0037-0040).

Regarding claim 17, Kimura discloses wherein the number generator is a pseudorandom number generator (Pages 3-4, Par. 0037-0040).

Regarding claim 21, Kimura discloses wherein the authentication is Wired Equivalent Privacy (WEP) authentication in accordance with Institute of Electrical and Electronics Engineers (IEEE) 802.11 (Pages 3-5, Par. 0037-0040 and 0054).

Regarding claim 22, Kimura discloses wherein a first predetermined number of initialization vectors associated with the first group is substantially less than a second predetermined number of initialization vectors associated with the second group (Pages 3-4, Par. 0037-0042).

Regarding claim 24, Kimura discloses an electronic device comprising: a memory to contain a plurality of keys including a shared secret key, a number generator, a device management logic in communication with the memory and the number generator, the device management logic including logic configured to analyze an initialization vector generated from the number generator to determine whether the initialization vector is used for either wired authentication or data communications, and a wireless transceiver to transmit and receive information for configured to support the authentication (Pages 3-4, Par. 0037-0042).

Regarding claim 23, Kimura discloses wherein the data communications include wired equivalent privacy (WEP) encryption and WEP decryption operations (Pages 3-4, Par. 0037-0040).

Regarding claim 25, Kimura discloses wherein the authentication is Wired Equivalent Privacy (WEP) authentication (Pages 3-4, Par. 0037-0040).

Regarding claim 26, Kimura discloses the electronic device of claim 24 is an access point (Page 2, Par. 0019).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 9-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kimura, (U.S. Publication No. 2001/0048744 and Kimura hereinafter), in view of Ala-Laurila et al., (U.S. Publication No. 2002/0009199 and Laurila hereinafter).

Regarding claim 9, Kimura does not expressly disclose wherein the determining whether the initialization vector falls within the first group includes determining whether a selected series of bits of the initialization vector has been set.

However, Laurila discloses wherein the determining whether the initialization vector falls within the first group includes determining whether a selected series of bits of the initialization vector has been set (Page 5, Par. 0051-0053).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Kimura with the teachings of Laurila because it would allow to include wherein the determining whether the initialization vector falls within the first group includes determining whether a selected series of bits of the initialization vector has been set with the motivation to ensure the reliability of the mobile network (Laurila, Page 1, Par. 0008).

Regarding claim 10, Kimura does not expressly disclose wherein the selected series of bits is continuous.

However, Laurila discloses wherein the selected series of bits is continuous (Page 5, Par. 0051-0053).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Kimura with the teachings of Laurila because it would allow to include wherein the selected series of bits is continuous with the motivation to ensure the reliability of the mobile network (Laurila, Page 1, Par. 0008).

Claims 20, and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kimura, (U.S. Publication No. 2001/0048744 and Kimura hereinafter), in view of Windel, (EP 862143A and Windel hereinafter).

Regarding claims 20 and 28, Kimura discloses a method comprising: selecting a bit size (N) of an initialization vector, and using an initialization vector from the second group exclusively for data communications.

Kimura does not expressly disclose partitioning all 2N initialization vectors into a first group and a second group, and using an initialization vector from the first group exclusively for authentication.

However, Windel discloses partitioning all 2N initialization vectors into a first group and a second group, and using an initialization vector from the first group exclusively for authentication (Abstract).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Kimura with the teachings of Laurila because it would allow to include wherein the selected series of bits is continuous with the motivation to obtain the output vector selected as a data authentication code for the data (Windel, Abstract).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (703) 305-8749. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax

phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Arezoo Sherkat
Patent Examiner
Group 2131
July 9, 2004

AVAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100